

CDSL/OPS/DP/POLCY/2025/27

January 10, 2025

IMMEDIATE CYBER INCIDENT & QUARTERLY CYBER INCIDENT REPORTING BY DPs

DPs are advised to refer to SEBI circular No: SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022, wherein all Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock brokers / Depositories Participants shall be reported to **Stock Exchanges / Depositories & SEBI** within 6 hours of noticing / detecting such incidents.

In view of the above, Depository Participants are hereby informed that CDSL has developed a facility for online submission of cyber incident reporting through audit web portal. Depository Participants shall also report about such incidents to CDSL through the dedicated e-mail id: <u>dpincident@cdslindia.com</u>.

For submitting the **immediate cyber incident report** to Stock Exchanges / Depositories, please refer **Annexure A.**

Further the incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Stockbrokers / Depository Participants, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

In addition to this, Stock Brokers / Depository Participants **must submit mandatory quarterly reports** to Stock Exchanges / Depositories on cyber-attacks, threats, incidents, breaches, and mitigation measures, including useful information on vulnerabilities, **within 15 days after the end of each quarter** i.e. Apr-June **(Q1)**, Jul-Sep **(Q2)**, Oct-Dec **(Q3)**, Jan-Mar **(Q4)**.

For submitting the **quarterly cyber incident report** to Stock Exchanges / Depositories, please refer **Annexure B.**



Queries regarding this communiqué may be addressed to: CDSL – Helpdesk Emails may be sent to: <u>dprtasupport@cdslindia.com</u> and connect through our IVR Number 022-62343333.

For and on behalf of Central Depository Services (India) Limited

sd/-

Akhil Wadhavkar Vice President– Information Technology



Annexure A

Guidelines to submit Immediate Cyber Incident Report

- 1. Open the Audit Web Portal.
 - Link: <u>https://auditweb.cdslindia.com/Login.aspx</u>
 - Click on Login Type and select "Designated Officer" login.

Audi	t Application
	Sign In
🏠 Login Type	Designated Officer
🧞 User ID	Select Auditor
Q Password	DP RTA CDSL_Staff
	De signated Officer CISA_Auditor
	Auction Committee Bidding Participant IS_Auditor
	DP_Admin RTA_Admin General_Admin
Forgot password	Registration for DP / RTA

- 2. Fill the below required information and click on "Sign In" Button:
 - User ID , Password & Captcha

Audi	T APPLICATION		
	Sign In		
🏫 Login Type	Designated Officer	~	
🧞 User ID	741910_ks		
🍳 Password	•••••		
	7afff1 🗘		
	7afff1		
	Sign In		
Forgot password	Registration for DP / RTA		



COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

- **3.** Enter the OTP:
 - You will receive the OTP on both your DP's registered mobile number and email Id.

Central Depository Services (India) Limited
AUDIT APPLICATION
LOGIN OTP Enter OTP OTP Time :- 00:09:57 Verify OTP
Copyright 💿 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

- 4. Select required information for submitting immediate "Cyber Incident" report:
 - Select Audit Type: CYBER MULTIPLE INCIDENT REPORT
 - Select Audit Month: Select the current month
 - Select DP/RTA: Select your DP ID
 - Click on the "**Confirm**" Button





COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

5. The following screen will appear. Main DP can mention the branch DP IDs, if they are submitting consolidated report for branch DP IDs.

		AUDIT APPLICATION		
CYBER INCIDENT REP	ORT			
Audit Type	CYBER INCIDENT REPORT	DP Name(ID)	74 Lii	
Audit Month	202403	Period	Jan-2024 to Mar-2024	
DP ID	74			

- 6. Fill in the details in the prescribed format in:
 - 1. Letter/Report Subject
 - 2. Reporting Periodicity Year
 - 3. Designated Officers details.

		Incident Repo	orting Form		
. Letter/Report Subject					
ame of the Depository Participant	7410		UNIQUE INCIDENT NO. :-	1	
ame of Depository	CDSL		Financial Year = 2024-2	2025	
IEMBER ID / DP ID	741				
. Reporting Periodicity Year					
uarter 4 [Jan-2024 to Mar-20	24]				
3. Designated Officer (Reporting	Officer details)				_
NAME	Name		* ORGANIZATION	Organization name	
TITLE	Title		* EMAIL ID	Email ID	
Phone / Fax No.	Phone / Fax No		* Mobile	Mobile	
Address	Address				
		1.			

- **7.** Select the option **Yes** in Cyber-attack/breach observed in Quarter and fill the below required information:
 - Date & Time
 - Brief information on the Cyber attack
 - Then Click on Annexure I



COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Cyber-attack / breach observed in	Quarter
E Yes 🗆 No	(IF ves, please fill Annexure I) (IF no, please submit the NIL report only after the end of quarter)
* Дате & Тіме	10-Jul-2024 04 15 V PM v (Select the Date between 01-Jan-2024 To 31-Mar-2024)
* Brief information on the Cyber attack / breach observed	Brief information on the Cyber-attack
Annexure I	

8. Fill the relevant details in Annexure I:

- 1. Physical location of affected computer/ Network and name of ISP
- 2. Date incident occurred
- 3. Information of affected system
- 4. Select the type/types of incidents
- 5. Description of incident

Physical location of affected con	nputer / Network and name of ISP						•	
2. Date incident occurred							//)	
Occured		Hour V Minutes V PM velocit the Date between 0	✔ * 1-Jan-2024 To 31-Mar-2024)					
IDENTIFIED	dd-MMM-yyyy	Hour V Minutes V PM V	~ •					
3. Information of affected syste	m							
IP Address	IP Address	Co	mputer / Host name		Computer / H	lost Name		
LAST PATCHED / UPDATED	dd-MMM-уууу	Ор	perating System (incl. Ver / release no.)	Operating Sys	stem		
Hardware Vendor / Model	Hardware model							
47 0 11 1								
4. Type of incident		_	DISTRIBUTED DENIAL OF SERVICE(DDOS)		NGINEERING	RANSOMWARE		
Type of incident PHISHING	□ WEBSITE DEFACEMENT	BOT/BOTNET	DISTRIBUTED DENIAL OF SERVICE(DDOS)					
		BOT/BOTNET EMAIL SPOOFING	User Account Compromise		al Vulnerability			
4. Type of incident		_			NGINEERING	RANSOMWARE		

- **9.** Fill the below Information:
 - Select Unusual behaviour/symptoms (Tick the symptoms)
 - Fill the Details of unusual behaviour/symptoms
 - Has this problem been experienced earlier? If Yes, Give the description



System crashes	Changes in file lengths or dates	
New user accounts/ Accounting discrepancies	ATTEMPTS TO WRITE TO SYSTEM	
Failed or successful social engineering attempts	DATA MODIFICATION OR DELETION	
UNEXPLAINED, FOOR SYSTEM PERFORMANCE	DENIAL OF SERVICE	
UNACCOUNTED FOR CHANGES IN THE DNS TABLES, ROUTER RULES, OR FIREWALL RULES	DOOR KNOB RATTLING	
UNEXPLAINED ELEVATION OR USE OF PRIVILEGES OPERATION OF A PROGRAM OR SNIFFER DEVICE TO CAPTURE NETWORK TRAFFIC	UNUSUAL TIME OF USAGE	
An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user	UNUSUAL USAGE PATTERNS	
A system alarm or similar indication from an intrusion detection tool	UNUSUAL LOG FILE ENTRIES	
Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	Presence of new setuid or setuid files Changes in system directories and files	
Anomalies	PRESENCE OF CRACKING UTILITIES	
Suspicious probes	ACTIVITY DURING NON-WORKING HOURS OR HOLIDAYS	
SUSPICIOUS EROWSING NEW FILES	Other	
Details of unusual behavior/symptoms		
Details of unusual behavior		
as this problem been experienced earlier? If Yes, details 🛛 Yes 🖾 No		

10. Fill the below Information:

- Agencies notified
- IP Address of apparent or suspected source
- How many host(s) are affected?

9. Agencies notified				
LAW ENFORCEMENT	Law Enforcement	Private Agency	Private Agency	
Affected Product Vendor		Other		
10. IP Address of apparent or	suspected source			
Source IP address		OTHER INFORMATION AVAILABLE		
11. How many host(s) are affe	cted?			
🗌 1 то 10 🗌 10 то 100 🗌 М	ORE THAN 100			
12. Details of actions taken fo	r mitigation and any preventive meas	ure applied		
	Clear Attach Files			
Save Submit to CDSL				

DPs can also save the multiple incidents in quarterly incident report module in audit web portal. After reporting each incident, please enter the "Save" button & add another incident if any. After entering all the incidents, please enter the Submit to CDSL.

Attach Files: Click "Attach Files" to upload relevant documents.
Save: Click "Save" to save your information as a draft.
Submit to CDSL: Click "Submit to CDSL" to officially submit your report.
Clear: Click "Clear" to remove all entered data and reset the form.



Annexure B

Guidelines to submit Quarterly Cyber Incident Report

- **1.** Open the Audit Web Portal.
 - Link: https://auditweb.cdslindia.com/Login.aspx
 - Click on Login Type and select "Designated Officer" login.

Aud	IT APPLICATION
	Sign In
🏠 Login Type	Designated Officer 🗸
Sour ID	Select Auditor
Q Password	DP RTA CDSL_Staff
	De signated Officer CISA_Auditor
	Auction Committee Bidding Participant
	IS_Auditor DP_Admin
	RTA_Admin General_Admin
Forgot password	Registration for DP / RTA

- 2. Fill the below required information and click on "Sign In" Button:
 - User ID, Password & Captcha

Aud	IT APPLICATION	
	SIGN IN	
🏠 Login Type	Designated Officer 🗸	
🧞 User ID	741910_ks	
Q Password	•••••	
	7afff1 🗘	
	7afff1	
	Sign In	
Forgot password	Registration for DP / RTA	

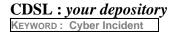


- **3.** Enter the OTP:
 - You will receive the OTP on both your DP's registered mobile number and email Id.

٠¢٠	Central Depository Services (India) Limited
	AUDIT APPLICATION
	LOGIN OTP Enter OTP Enter OTP OTP Time :- 00:09:57 Prest of each the page Verify OTP
Copyright © 20	019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

- 4. Select required information for submitting quarterly "Cyber Incident" report:
 - Select Audit Type: CYBER INCIDENT REPORT
 - Select Audit Month: Select quarter month
 - Select DP/RTA: Select your DP ID
 - Click on the "**Confirm**" Button

		AUDIT APPLICATION			
	Reports				
	Select Audit Type	CYBER INCIDENT	T REPORT	~	
	Select Audit Month	September-	2022	~	
	Select DP / RTA	74	þ	~	
		Confir	m		
		View Cyber Report VAPT Compl Cyber Audit Compliance Repo			
		System Audit Com	pliance Report		
		Go to Login Cha	nge Password		
٨Q					





5. The following screen will appear. Main DP can mention the branch DP IDs , if they are submitting consolidated report for branch DP IDs.

		AUDIT APPLICATION		
CYBER INCIDENT REP	ORT			
Audit Type	74 Lit			
Audit Month	202403	Period	Jan-2024 to Mar-2024	
DP ID	74			

- 6. Fill in the details in the prescribed format in:
 - 1. Letter/Report Subject
 - 2. Reporting Periodicity Year
 - 3. Designated Officers details.

		Incident Repo	orting Form		
. Letter/Report Subject					
ame of the Depository Participant	7410		UNIQUE INCIDENT NO. :-	<u>.1</u>	
ame of Depository	CDSL		Financial Year = 2024-	2025	
IEMBER ID / DP ID	741				
. Reporting Periodicity Year					
uarter 4 [Jan-2024 to Mar-20	24]				
3. Designated Officer (Reporting	Officer details)				_
NAME	Name		* Organization	Organization name	
Τιτιε	Title		* EMAIL ID	Email ID	
Phone / Fax No.	Phone / Fax No		* MOBILE	Mobile	
Address	Address				

7. Select the option NO in Cyber-attack/breach observed in Quarter: (If no incident has occurred)



Convenient + Dependable + Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

Cyber-attack / breach observed in	(IF yes, please fill Annexure I) (IF no, please submit the NIL report only after the end of quarter)
Date & Time	[dd-MMM-yyyy] [Hour ▼] [Minutes ▼] [PM ▼] (Select the Date between 01-Jul-2023 To 30-Sep-2023)
Brief information on the Cyber attack / breach observed	Brief information on the Cyber-attack
Annexure I	

The Report is submitted as NIL report.

- 8. Select the option Yes in Cyber-attack/breach observed in Quarter and fill the below required information: (if the incident occurred)
 - Date & Time
 - Brief information on the Cyber attack
 - Then Click on Annexure I

🛚 Yes 🗆 No	(IF YES, PLEASE FILL ANNEXURE I) (IF NO, PLEASE SUBMIT THE NIL REPORT ONLY AFTER THE END OF QUARTER)
* Date & Time	[10-Jul-2024] [04 ♥] [15 ♥] [PM ♥] (Select the Date between 01-Jan-2024 To 31-Mar-2024)
* Brief information on the Cyber attack / breach observed	Brief information on the Cyber-attack

9. Fill the Annexure I:

- 6. Physical location of affected computer/ Network and name of ISP
- 7. Date incident occurred
- 8. Information of affected system
- 9. Select the type/types of incidents
- 10. Description of incident



COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

1. Physical location of affected co	omputer / Network and name of	ISP				
Physical location of affected comp	outer / Network and name of ISP					•
2. Date incident occurred						
Occured		Hour V Minutes V PM elect the Date between 0	▼ * 1-Jan-2024 To 31-Mar-2024)			
Identified	dd-MMM-yyyy	Hour 🗸 Minutes 🗸 PM	v *			
3. Information of affected system	n					
IP ADDRESS	IP Address	Co	DMPUTER / HOST NAME	Computer /	Host Name	
LAST PATCHED / UPDATED	dd-MMM-уууу	0	PERATING SYSTEM (INCL. VER / RELEASE NO.) Operating S	ystem	
Hardware Vendor / Model	Hardware model					
4. Type of incident						
	□ WEBSITE DEFACEMENT	Вот/Вотнет	DISTRIBUTED DENIAL OF SERVICE(DDOS)	SOCIAL ENGINEERING	RANSOMWARE	
NETWORK SCANNING / PROBING BREAK	IK-IN/ROOT 🗌 SYSTEM MISUSE	EMAIL SPOOFING	USER ACCOUNT COMPROMISE	TECHNICAL VULNERABILITY	OTHER	
VIRUS/MALICIOUS CODE	SPAM	DENIAL OF SERVICE(DOS)	WEBSITE INTRUSION	IP Spoofing		
5. Description of Incident						
Description of incident						

10. Fill the below Information:

- Select Unusual behaviour/symptoms (Tick the symptoms)
- Fill the Details of unusual behaviour/symptoms
- Has this problem been experienced earlier? If Yes, Give the description

	System crashes	Changes in file lengths or dates	
UnickPrivation processified Presonance District or Statistics UnickCounted proc statistics counter Roules, con Frakewall Roules Door Roude Battlinic UnickCounted proc statistics, Bourter Roules, con Frakewall Roules Door Roude Battlinic UnickCounted proc statistics, Bourter Roules, con Frakewall Roules Door Roude Battlinic Namescation of a vesse account That Door Shore Coeresponde Do The Actival Later The Or Unicade To The Shore Divisious The Or Unicade Do Tubes Roor Coeresponde Do The Actival Later The Or Unicade To The Unice Do Tubes Roor Coeresponde Do The Actival Later The Or Unicade To The Unice Do Tubes Roor Coeresponde Do To The Actival Later The Or Unicade To The Unice Do Tubes Roor Coeresponde Do To The Actival Later The Or Unice Do Tubes Roor Coeresponde Do To The Actival Later The Or Unice Do Tubes Roor Coeresponde Do To The Actival Later The Or Unice Do Tubes Roor Coeresponde Do To The Actival Later The Or Unice Do Tubes Roor Coeresponde Do To The Activate Do Tubes Roor Coeresponde Roor Coeresponde Do Tubes Roor Coeresponde Roor Coeresponde Roor Coeresponde Do Tubes Roor Coeresponde Do Tubes Roor Co	New user accounts/ Accounting discrepancies	ATTEMPTS TO WRITE TO SYSTEM	
Unaccount to por changes in the DNS tables, notifie Rules, or presental Rules Doe Rules and failing Underdianted pick changes in the DNS tables, notifie Rules, or presental Rules Underdianted or use or previncies Oreaction or a prededum or sinifier botic to cartie en network tabler? Underdianted or use or previncies Oreaction or a prededum or sinifier botic to cartie en network tabler? An indicated Last Thile or uses a cocount that does not cocketspendo to the actual Last Thile or uses all core interes Underdianted An indicated Last Thile or uses a cocount that does not cocketspendo to the actual Last Thile or uses all core interes Individual de partients An indicated use similar indication an intresion or treed and interestion or the Actual Last Thile or uses all core interestion or station on List Changes in system directories and presented or a set similar indication or set account that does indication or the Actual Last Thile or uses all core interestion or set account that does indication or set account or unit interestion or interestion or interestion or interestion or interestion or interestic or interestic or interestic or interestic interestic or interestic interestic or interestic or interestic interestic or interestic or interestic interestic or interestic interestic or interestic interestinterestic interestic interestic interestic int	Failed or successful social engineering attempts	Data modification or deletion	
Unstructure of used of privileges Operation of a procedum of shifter brive to to cartiere nitwork teatric Unstructure or used An indicated Last Time or used of a user account that boos not correspond to thi actual Last Time or used for thirts Unstructure is A indicated Last Time or used of a user account that boos not correspond to thi actual Last Time or used for thirts Unstructure is A indicated Last Time or used to a user account that boos not correspond to thi actual Last Time or used for thirts Unstructure is Attende os simile in indication rison an intrusion effection tool Unstructure is thirts Attende rises, which are usually the intrustion attender for usually on on the Pages on the Wes served Pretence or eacties or runtifies Subjections radies On construction or used is on usual pretence or eacties or runtifies Subjections radies Activity publies non-working non-worki	UNEXPLAINED, POOR SYSTEM PERFORMANCE	Denial of service	
An INDICATED LAST TIME OF USAGE OF A USEE ACCOUNT THAT DOES NOT CORRESPOND TO THE ACTUAL LAST TIME OF USAGE FOR THAT USE A DIVENUE AGE OF A USEE ACCOUNT THAT DOES NOT CORRESPOND TO THE ACTUAL LAST TIME OF USAGE FOR THAT USE I UNUSUAL LOS FLE ENTERIS ALAMM OR SIMILAR INDICATION AN INTEUSION DETECTION TOOL ATTERD HOME FAGES, WHICH ARE USUALLY THE INTENTIONAL TARGET FOR VISUALLY, OR OTHER PAGES ON THE WEB SERVER I PRESENCE OF CRACKING VILLITES ANDMALIES SUSPICIOUS FROESS SUSPICIOUS FROESS I COLUMN FROE AND INTELS I C	Unaccounted for changes in the DNS tables, router rules, or firewall rules	DOOR KNOB RATTLING	
A system ALARM OK SINILAR INDIKATION FROM AN INTRUSION RETECTION TOOL Unussual Loo File ENTRIES Attracto Houle PAGES, WHIch ARE USUALLY THE INTENTIONAL TAGET FOR WISHILITY, OK OTHER PAGES ON THE WEB SERVER Pesetence OF NEW SErvice OF NEW SER	Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic	UNUSUAL TIME OF USAGE	
Attekto Home PAGE, which Ake USJALLY The INTENTIONAL TARGET FOR VISIBILITY, OR OTHER PAGES ON THE WEB SKRVER PRESEnce OF NEW SETUID OR SETUI	An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user	UNUSUAL USAGE PATTERNS	
Anomatilis Presence or cracking utilities Superiorus rotess Activity obeling how-workting Houss or Houbavs Superiorus rotess Other	A SYSTEM ALARM OR SIMILAR INDICATION FROM AN INTRUSION DETECTION TOOL	UNUSUAL LOG FILE ENTRIES	
Supericous Process Activity outeline Non-working Houldays Supericous process Other	Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	PRESENCE OF NEW SETUID OR SETGID FILES CHANGES IN SYSTEM DIRECTORIES AND FILES	
Sussections Rew Files OTHER tails of unusual behavior/symptoms	Anomalies	PRESENCE OF CRACKING UTILITIES	
tails of unusual behavior/symptoms	Suspicious probes	ACTIVITY DURING NON-WORKING HOURS OF HOLIDAYS	
	Suspicious browsing New files	C OTHER	
alls of unusual behavior	tails of unusual behavior/symptoms		
	ails of unusual behavior		
s this problem been experienced earlier? If Yes, details 💿 Yes 🖾 No			

- **11.** Fill the below Information:
 - Agencies notified
 - IP Address of apparent or suspected source
 - How many host(s) are affected?



9. Agencies notified			
LAW ENFORCEMENT	Law Enforcement	Private Agency	Private Agency
Affected Product Vendor		Other	
10. IP Address of apparent or susp	ected source		
Source IP address		OTHER INFORMATION AVAILABLE	
11. How many host(s) are affected	?		
🗆 1 то 10 🗆 10 то 100 🗆 Моге	than 100		
12. Details of actions taken for mit	igation and any preventive measure applied		
			æ
Save Submit to CDSL Att	tach Files View Incident		

Attach Files: Click "Attach Files" to upload relevant documents.

Save: Click "Save" to save your information as a draft.

testaudit.cdsl.co.in says Records Added Sucessfully!!!	

Submit to CDSL: Click "Submit to CDSL" to officially submit your report.

testaudit.cdsl.co.in says Cyber Incident report submitted to CDSL 111
--

View Incident: Click "**View Incident**" to see your submitted reports history.

ANNEXURE I					
Save Submit to CDSL	Attach Files View Incident				
		Coovright @ 2019 - Audit Team, Central Depository Services (India) Ltd, All rights reserved.	1		

Note:

- All incidents report activities must be completed in one continuous action, from saving to submitting the incident sreport.
- Once you submit the incident report, it cannot be submitted again.
- When you re-login, the scheduled month/DP ID will not appear, that means you have already submitted the incident report.
